Mott Community College Acceptable Use Administrative Policy for Computers, Computer Networks, and Communication Systems
Effective July 1, 2009
Revised September 14, 2012

As an employee of Mott Community College, heretofore referred to as “The College,” all college employees are required to adhere to the following Acceptable Use Policy regarding the use of our computer, network, communications, and telephone equipment, heretofore referred to as “The Network”. Employees are defined as full-time, part-time, temporary and contracted faculty/staff. Employees do not include those individuals hired through the campus student employment program, heretofore referred to as “Student Employees”. This document functions in conjunction with related College Policy.

I. Employees’ right to privacy of communications when using The Network is not guaranteed. The College reserves the right to monitor all communications that use or are stored on The Network as it deems necessary.

II. All data, software programs, and information stored on The Network is the sole property of The College. Users must respect the legal protection of applied programs, data, photographs, music, written documents and other material as provided by copyright, trademark, patent, licensure and other proprietary rights, unless otherwise specifically excluded or modified in a collective bargaining agreement or written agreement between The College and The Employee. Student Employees shall not be granted account access to systems housing confidential student and personnel information, including but not limited to: ERP systems and supporting services, Data warehouse and Network Share Drives.

III. College employees will not use The Network to transmit any material (via e-mail, uploading, posting or otherwise) that does the following:
   a. Intentionally or unintentionally, violates any applicable local, state, national or international law, or conducting any activity that exposes The College to potential litigation or expenses or violates any other College rule or regulation
   b. Threatens or encourages bodily harm or destruction of property
   c. Harasses or discriminates against another person in any way or is harmful to students, employees, agents, or minors
   d. Is malicious, fraudulent or misrepresentative in purpose, including, but not limited to, spreading false information about a student, employee, agent, or minor
   e. Is related to pornography of any type or uses profanity, obscenity, discriminatory language, vulgarities or other inappropriate language or graphics.
   f. Is related to gambling

©Copyright 2012 Mott Community College
IV. The College is not responsible for damages or loss of personal files stored on The Network. Additionally, while attached to a College-owned computer, personal equipment may be subject to incidental access while the College is maintaining College-owned devices. For example, The College has the same authority to access a non-College-owned hard drive attached to College-owned equipment as they have for accessing College-owned equipment.

V. Employees must not use The Network or any other resources owned by The College for personal commercial purposes or financial gain. Employees must not excessively use the communications or telephone system for personal transactions.

VI. Employees are expected to take all necessary steps to safeguard Proprietary and Confidential Information that resides on the network from release to unauthorized parties. Proprietary Information includes, but is not limited to, College financial information and/or other information that could damage The College’s business should it be released to an unauthorized party. Confidential Information includes, but is not limited to, customer information, student information, employee information, and information relating to The College. This includes securing and safeguarding data stored on portable devices used to transport data, such as flash drives.

VII. Employees must not use The Network to knowingly distribute spam, chain letters or other mass unsolicited mailings.

VIII. Employees must not use The Network for any activity which adversely affects the ability of other people or systems to use The Network. This includes, but is not limited to:
   a. Denial of service attacks against another network by routing or relaying traffic between unknown third parties, worms, viruses or other intrusive services
   b. Interference with or disruption of other network users, services or equipment
   c. Through action or inaction, to allow The Network to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner
   d. Attempts to penetrate security measures of The Network via computer software, hardware or other systems whether or not the intrusion results in the corruption or loss of data
   e. Employees must not install or use game software, entertainment software, screen saver or any other software that interferes with The Network or their desktop computer unless necessary for their job function at The College
IX. Employees must respect the privacy of others and shall not intentionally seek information on, or represent themselves as another employee unless explicitly authorized to do so by that employee or supervisor.

X. Employees must not disclose any Login IDs or passwords to any person except as directed by their supervisor. Employees should never disclose their Login IDs or passwords for student use in any capacity under any circumstances. The authorized user of the account is responsible for all activities associated with the account.

XI. Employees are allowed to disseminate information using The Network under the following conditions:
   g. For Proprietary Information, employees must get permission from their supervisor before communicating this information to any third party, including verbal, written, or through The Network.
   h. For Confidential Information, employees must get permission from their supervisor before communicating this information to any third party, including verbal, written, or through The Network.

XII. Violations of the policies set forth in this document will result in disciplinary action in accordance with the appropriate Collective Bargaining Agreement clause(s) regarding disciplinary procedures. The resulting action may include but is not limited to the following: termination of use, written discipline, suspension, or termination of employment from The College and/or legal action taken against the Employee by The College. All investigations shall be conducted under the jurisdiction of the Office of Human Resources and/or an independent investigator if necessary.